REMARKS

Claims 7, 9-11, 13-17, and 19 are pending in this application. Claims 1-6, 12, 13 and 20 have been canceled without prejudice or disclaimer. Claim 11 has been amended. No new matter has been added.

Claim Rejections under 35 U.S.C. §101

Claims 5, 11-13 are rejected under 35 U.S.C. §101 as they recite a software program per se which is non-statutory subject matter. Claims 5 and 12-13 have been canceled without prejudice or disclaimer and claim 11 has been amended to overcome the rejection under 35 U.S.C. §101. Accordingly, the rejection should be withdrawn.

Claim Rejections under 35 U.S.C. §102

Claims 7, 9-11, 14-17, and 19 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,483,649 to Kuznetsov et al. Applicants request reconsideration of the rejection for the following reasons.

According to the present invention, an intrusion detection program 43 in a host 40 or a virus detection unit 44 thereof detects an event and a data protection unit 74 stops duplication or replication of data in a storage volume 64 that is duplicated in a duplication area 67, or as shown in Figure 7, in duplication areas 67a, 67b, and 67c. The replicated volume stores data duplicated from the storage volume. When an event is detected, the replication is stopped by instructing the control unit that controls the transfer from the storage volume to the replicated volume to stop data transfer. Further, the computer system detects an intrusion in the

computer and instructs the storage control unit to stop data transfer from the storage volume to the replicated volume when the intrusion is detected.

Claims 7, 9-11 and 14 are the independent claims. The invention of claim 7 sets forth a data protection apparatus for protecting data in a storage volume in a computer system, which includes a storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from the storage volume, and a storage control unit for controlling data transfer from the storage volume to the replicated volume. The data protection apparatus includes an event detection unit for detecting an event occurrence, and a replication stopping unit for instructing the storage control unit to stop data transfer from the storage volume to the replicated volume when the event detection unit detects an event. The computer system further includes a computer for reading and writing data from and to the storage volume, and an illegal intrusion detection unit for detecting an illegal intrusion into the computer. The event detection unit is able to receive a detection of the illegal intrusion from the illegal intrusion detection unit. When the event detection unit receives the detection of the illegal intrusion, the replication stopping unit instructs the storage control unit to stop data transfer from the storage volume to the replicated volume.

In independent claims 10 and 11, a data protection method and a program for making an information processing apparatus perform data protection are claimed for a storage volume in a computer system, in which the computer system includes a storage volume assigned for storing data, a computer for reading and writing data from and to the storage volume, a replicated volume assigned for storing data duplicated from the storage volume, and a storage control unit for controlling data transfer from the storage volume to the replicated volume.

The data protection method or process steps that are performed include detecting an intrusion into the computer, and instructing the storage control unit to stop data transfer from the storage volume to the replicated volume, when the intrusion is detected.

In claim 14 a computer system is claimed that includes a storage volume assigned for storing data, a replicated volume assigned for storing data duplicated from the storage volume, a storage control unit for controlling data transfer from the storage volume to the replicated volume, and a data protection apparatus for protecting data in the storage volume. The data protection apparatus includes an event detection unit for detecting an event occurrence, and a replication stopping unit for instructing the storage control unit to stop data transfer from the storage volume to the replicated volume, when the event detection unit detects an event. The computer system further includes an alteration detection unit that reads given data in the plurality of replicated volumes to detect respective differences between the given data. The event detected by the event detection unit is a detection result of the differences between the given data, with the detection result being received from the alteration detection unit.

Kuznetsov et al. is relied upon for disclosing a personal computer subsystem having a hardware module and protection software including a protection-program support module 120B that protects files on a personal computer from inadvertent or intentional distortion. The module blocks access paths to a hard disk controller 30, which controls hard disk 32, when "dangerous requests" are detected. A dangerous request includes hard disk 32 formatting requests, write requests not preceded by use of the modular device driver 26, and write requests from sources other than the modular device driver 26. See column 7, lines 40-

50 of the reference. However, Kuznetsov is not directed to a computer system including a storage volume assigned for storing data and a replicated volume assigned for storing data duplicated forms the storage volume, to which the present invention is directed. Accordingly, although the reference discloses blocking path access from a personal computer to a hard disk when a dangerous request is detected, the present invention is different and not obvious from Kuznetsov.

The Applicants recognize that a Trojan horse may be planted or a back door opened or an infection with a computer virus may occur before the intrusion detection unit 43 or the virus detection unit 44 detects the event, making it difficult to protect the storage volume 64 by disconnecting the path between the host 40 and the storage volume 64. Rather, when the data protection unit 74 executes a data detection program, the reflection, duplication or replication of data from the storage volume 64 onto the replicated volume 67 or volumes 67a, 67b or 67c, is stopped. This enables the data held in the storage volume 64 at the time before the event has been detected to be secured in the replicated volume(s). That is , the data held in the storage volume 64 before the computer event occurs against the host 40 is detected and the duplication of data between the storage volume 64 and the replicated volume 67 is stopped. See page 19, lines 3-8 of the specification.

Specifically, as shown in Figure 7, as a result of a transfer delay unit 66 or through a controller that instructs the replication to occur with respective time differences, replicated volume(s) 67 or 67a-67c hold respective snapshots of the storage volume 64 with a time difference that secures the data in the duplicated areas from being affected by the event detected by the intrusion detecting program or virus detection software. As set forth in claim

15, write data of the storage volume is transferred by the storage control unit to the replicated volume with a delay of a given time. Further, according to claim 16, a plurality of replicated volumes are set forth and the storage control unit switches a transfer destination of the write data of the storage volume, at given time intervals among said plurality of replicated volumes. The Since the Kuznetsov reference does not disclose the duplication of a primary volume to a replicated volume, there is not disclosure or suggestion in the reference stopping the replication of data in order to secure data in duplicated areas, as in the present invention. Accordingly, the rejection under 35 U.S.C. §102 should be withdrawn.

CONCLUSION

In view of the foregoing, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

By _____
John R. Mattingly
Reg. No. 30,293
(703) 684-1120

JRM/so
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
703-684-1120
Date: May 17, 2006